APPELLANTS' BRIEF ON APPEAL

John F. Vodopia
Attorney for Appellants
Reg. No. 36,299

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza-Suite 300
Garden City, New York 11530
(516) 742-4343

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Morton G. Swimmer, et al.

Examiner: Courtney D. Fields

Serial No.: 10/791,992

Art Unit: 2137

Filed: March 3, 2004

Docket: CH920020050US1(20960)

For: DATA PROCESSING SYSTEM

Dated: February 11, 2008

Confirmation No.: 4840

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 2233-1450

APPEAL BRIEF

Sir:

Pursuant to 35 USC § 134 and 37 CFR §41.37, entry of Appellants' Appeal Brief, provided in support of Appellants' Notice of Appeal dated December 17, 2007, is respectfully requested.

The Appeal Brief sets forth the authorities and arguments upon which Appellants rely in support of their Appeal from the final rejection of all of the pending claims 1-23 over the asserted prior art, where the final rejection was set forth in a final Office Action mailed September 7, 2007, in the above-identified application.

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent & Trademark Office via Electronic Filing through the United States Patent and Trademark Office e-business website, on February 11, 2008.

Dated: February 11, 2008

John F. Vodopia, Esq.

I. REAL PARTY IN INTEREST

The real party in interest of the present application is International Business Machines Corporation, the assignee of the entire right, title and interest in the above-identified patent application.

II. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known which directly affect, or will be directly affected by, or have a bearing on, the disposition of the pending appeal.

III. STATUS OF THE CLAIMS

The claims argued on appeal are claims 1-23. The status of claims 1-23 on appeal is as follows:

Claim 1-23 stand rejected under 35 USC 102(e) in view of US Patent No. 5,414,844 to Wang.

IV. STATUS OF AMENDMENTS

In response the final Office Action mailed September 7, 2007 ("the final Office Action"), Appellants filed an Amendment Under 37 CFR 1.116, on November 7, 2007 ("the final Amendment"). Claims 1-23 were finally rejected under 35 USC 102(e) in view of published US Patent No. 5,414,844 to Wang in the final Office Action.

An Advisory Action was mailed from the Patent Office on November 19, 2007 ("the Advisory Action"), which maintained the final rejection of all of claims 1-23. On December 17, 2007, appellants filed their Notice of Appeal.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1-23 are pending in this application, where claims 1 and 10 are the independent claims. Claims 2-9 and 20-22 depend from claim 1, and claims 11-19 and 23 depend from claim 10. A copy of the rejected claims is attached hereto in the Claims Appendix.

The invention of independent claim 1 sets forth a method for controlling access to an object in a data processing system (Specification at page 3, lines 17-19; Fig. 4) the method comprising:

receiving an access request to access the object from a task (Specification at page 12, lines 1-2; Fig. 4);

classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task (Specification at page 12, lines 2-6; Fig. 4);

granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class (Specification at page 12, lines 6-9; Fig. 4); and,

in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data (Specification at page 12, lines 10-19; Fig. 4).

The invention of independent claim 10 sets forth an apparatus for controlling access to an object in a data processing system (Specification at page 3, lines 17-19; Fig. 2; page 11, lines 14-16), the apparatus comprising:

an access control data store for storing access control data associated with the object and the task; an access log (Specification at page 11, lines 16-19; Figs. 2; memory subsystem 220);

access control logic for receiving a request to access the object from a task (Specification at page 11, lines 16-19; Figs. 2, 3, 6; access controller 280; access control logic 300, page 13, lines 5-25);

decision classifier logic, connected to the access control logic, the access control data store, and the access log, for classifying the access request into one of critical and non-critical classes in dependence on the access control data, and, in the event that the access is classified into the non-critical class, for granting the task access to the object and storing data indicative of the access in the access log (Specification at page 13, lines 5-25; decision classifier logic 310); and,

access control decision logic connected to the access control logic, the access log, the access control data store, and the decision classifier logic, for, in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the access control data (Specification at page 13, lines 5-25; access control decision logic 320).

The patentability of the dependent claims shall stand or fall based on the patentability of the independent claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-23 were finally rejected under 35 USC 102(e) in view of US Patent No. 5,414,844 to Wang by the final Office Action (dated September 7, 2007).

VII. ARGUMENT

A.) Wang does not render claims 1-23, unpatentable under 35 USC §102(e)

Appellants submit that the final rejection of claims 1-23 under 35 USC §102(e) in view of Wang is improper in view of the fact that Wang does not disclose Appellants' invention as claimed.

In the final Office Action, the rejection of Claims 1-23 under 35 USC §102(e) as anticipated by US Patent No. 5,414,844 to Wang was maintained (on final). With respect to independent Claims 1 and 10, the Examiner states therein that Wang discloses a method, apparatus and computer program product for controlling access to an object in a data processing system, including:

receiving an access request to access the object from a task (col. 5, lines 60-63);

classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task (col. 5, line 66 through col. 6, line 8);

granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class (col. 6, lines 8-11); and,

in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data (col. 6, lines 12-23).

At page 12 of Appellants' specification, lines 1-19, Appellants describe the inventive operation with reference to Fig. 4. That is, on receipt of a request to access an object 250 from a task 270, at block 301 of Fig. 4, access controller 280 classifies the request, at block 302, into one of a critical and non-critical task in dependence on stored access control data 285, associated with the object and task. Access to a critically classed object is granted or denied in dependence on the content of access log 290 and the stored access control data 285.

Wang, as distinguished from Appellants' invention as claimed, teaches a method and system for controlling access to a plurality of data objects stored in a data processing system. The Wang method and system use an access control profile associated with each data object that includes an explicit authorization parameter listing user identities and authorization levels, a shared authorization parameter listing the identity of a plurality of users and authorization level granted to each listed user, and a public authorization parameter listing the authorization level granted to each user not specifically set forth in the access control profile.

A single public user identity is then defined for all users not specifically set forth within the access control profile. That identity as well as a public authorization level for an entire group of data objects is listed within a single shared authorization parameter. A reference to the shared authorization parameter is placed within the group so that public access to the entire group of data objects may be centrally controlled by means of a single shared authorization parameter.

Significantly, the Court of Appeals for the Federal Circuit emphasizes that a strict identity test must be met in order for a reference to anticipate a claim under 35 U.S.C. 102. For instance, in Apple Computer, Inc. v. Articulate Systems, Inc., 57 USPQ2d 1057, 1061 (Fed. Cir 2000), the Court explained that: "[a]nticipation under 35 U.S.C. 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." "Substantial identity" or "equivalency" is not sufficient. RCA Corp. V. Applied Digital Data Sys., Inc., 221 USPQ 385 (Fed. Cir. 1984). Appellants respectfully assert that neither the final Office Action nor the Advisory Action establish that Wang includes each limitation of the invention as set forth in independent claims 1 and 10, and the claims depending therefrom under the law.

Wang's Specification at col. 5, lines 63, through col. 6, line 23, describes Wang's access control. At col. 5, lines 66-col. 6, line 11, Wang states: "[a]fter access of a particular document has been requested, as determined in block 82, block 84 illustrates a determination of whether or not the user requesting access is a listed user. By 'listed user' what is meant is a user whose identity is specifically set forth within access control model object (ACMO) for the document in question. If the user requesting access to the document is a listed user, as determined in block 84, block 86 illustrates a determination of whether or not the user in question possesses a sufficient authority level for the action desired. If not, an error message is returned, as illustrated in block 88. If the user in question has sufficient authority level for the action desired, then access is granted, as depicted in block 90."

While the Examiner asserts that Wang discloses classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task, at col. 5, line 66-col. 6, line 8, Appellants respectfully disagree. The cited Wang text merely states that Wang determines whether or not a user requesting access is a listed user, as set forth in an ACMO. Block 84 determines whether the user is a listed user, and block 86 determines the user's authority level. As already mentioned, Wang utilizes a method by which public access to a large group of data objects is centrally controlled by use of data object 40 to classify access to one of two classes in association with the user, or user's role for access. Some users can read an object, and some users can write to an object. Nowhere does Wang disclose classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task.

While the Examiner asserts that Wang discloses granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class, at col. 6, lines 8-11, Appellants again respectfully disagree. The cited text does not support the Examiner's position. That is, at col. 6, lines 8-11, Wang merely states that if a user in question does not have sufficient authority to access a requested document or object, access to the document is denied, and if the user has sufficient authority, access is granted. Wang's users must meet the requirements for determining authority level for accessing an object classified in a critical class to gain access using a shared authorization parameter. Wang's disclosed structure and operation is not equivalent to granting or denying access to the object by the task in dependence on contents of Appellants' claimed access log if access is classified into the non-critical class. Wang teaches role-based access.

Further, while the Examiner asserts that Wang teaches that in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data (col. 6, lines 12-23), Appellants again respectfully disagree. The cited Wang text merely states, with respect to block 84 that if a user attempting to access is not a user specifically set forth in a ACMO for the document in question access is denied, and block 94 determines whether a public authority parameter includes a reference to a shared authority parameter. That is, if the user attempting access is not listed in the ACMO, an error is returned and access denied. And if the user is listed as OK-ed for access, access is limited by the shared authorization parameter.

In the "Response to Arguments," at paragraphs 3-7 of the final Office Action, and in the "continuation of 11" in the Advisory Action, the Examiner explains the reasoning behind the final rejection of claims 1-23 under section 102(e) in view of Wang, and why Appellants' arguments presented in response to the March 9, 2007 Office Action, and the final Office Action were deemed not to have overcome the rejections.

In particular at paragraph 4 "Response to Arguments," in the final Office Action, the Examiner states that Wang, contrary to Appellants' assertion, discloses the step of classifying an access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task, at col. 4, lines 59-67, col. 5, lines 1-7. The Examiner reiterates same argument in the continuation of 11 in the Advisory Action.

Applicants again disagree with the Examiner's stated position. At col. 4, lines 59-67, Wang states: that public authorization parameter 52 may include reference to shared authorization parameter 50, shown in detail at reference numeral 54, and includes a column of user identities 56 and associated authority level for each user in column 58. A user A is authorized to read library object 42 and other library object which includes shared authorization parameter 50 in its associated ACMO. At col. 5, lines 1-7, Wang states: that a user B is authorized to write into library object 42, as well as any other library object which includes shared authorization parameter 50 within its associated ACMO. In a like manner, a user C is permitted unlimited authority with regard to library object 42 and any other including shared authorization parameter 50.

Appellants do not read the cited text as teaching or suggesting classifying an access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task.

In particular at paragraph 5 "Response to Arguments," in the final Office Action, the Examiner asserts that Wang teaches the step of granting task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class, at col. 3, lines 59-67, col. 4, lines 1-8. The Examiner reiterates same argument in the continuation of 11 in the (November 19, 2007) Advisory Action.

At col. 3, line 59-col. 4, line 8, Wang states: that it is often important for users within one portion of the distributed data processing network 8 to access a data object or document stored in another portion of the network, and that to maintain order within the stored documents, it is desirable to have access control. Wang continues that this task is accomplished by listing those users authorized to access each data object or document, along with the level of authority that each user enjoys, and that it is well known to permit a group of users (a role-based class) to access a particular document by identifying a user, and level of the user's authorization permitted, in a shared authorization parameter stored within an access control profile associated with multiple data objects or documents.

The cited text does not teach or suggest granting task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class.

In particular at paragraph 6 "Response to Arguments," in the final Office Action, the Examiner asserts that Wang teaches that in the event that the access is classified into a critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data, at col. 6, lines 12-23. The Examiner reiterates same argument in the continuation of 11 in the (November 19, 2007) Advisory Action.

The cited Wang text merely states that, with respect to block 84, that if a user attempting to access is not a user specifically set forth in a ACMO for the document in question, block 94 determines whether a public authority parameter includes a reference to a shared authority parameter. If the user attempting access is not listed in the ACMO, an error is returned and access denied. And if the user is listed as OK-ed for access, access is limited by the shared authorization parameter.

The cited Wang text does not teach or suggest that in the event that the access is classified into a critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data.

B.) Conclusion

Appellants, therefore, respectfully assert that independent claims 1 and 10 are not anticipated by Wang for at least the reasons set forth, and urge the Board of Patent Appeals to overturn the final rejection of claims 1 and 10 under Section 102(e) in view of Wang. Claims 2-9 and 20-22 depend from claim 1, and are patentable therewith. Likewise, claims 11-19 and 23 depend from claim 10, and are patentable therewith. Appellants' further request that the Board overturns the rejections of claims 2-9 and 11-23 under Section 102(e) in view of Wang, and allows all of pending claims 1-23.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection herewith to Deposit Account No. 19-1013/SSMP.

Respectfully submitted,

John F. Vodopia
Registration No.: 36,299
Attorney for Appellants

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

Enclosures: Appendices VIII, IX and X

VIII. CLAIMS APPENDIX

1. (Original) A method for controlling access to an object in a data processing system, the method comprising:

receiving an access request to access the object from a task;

classifying the access request into one of critical and non-critical classes in dependence on stored access control data associated with the object and the task;

granting the task access to the object and storing data indicative of the access in an access log if the access is classified into the non-critical class; and,

in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the stored access control data.

2. (Original) A method as recited in Claim 1, further comprising, in the event that the access is classified into the non-critical class, granting or denying the task access to the object in dependence on the access control data, and storing data indicative of the grant or denial in the access log.

3. (Original) A method as recited in Claim 1, wherein the non-critical class comprises a plurality of subclasses and the classifying comprises classifying the access request into one of the subclasses in dependence on the stored access control data.

4. (Original) A method as recited in Claim 1, wherein the subclasses comprise a first subclass and a second subclass.

5. (Original) A method as recited in Claim 4, further comprising storing recovery data in the access log if the access is classified into the second subclass.

6. (Original) A method as recited in Claim 5, further comprising:

inspecting the access log to identify a bad grant decision based on the contents of the access log and the access control data; and,

on detection of a bad grant decision, rolling back any objects affected by the bad grant decision.

7. (Original) A method as recited in Claim 6, wherein the rolling back comprises recovering data overwritten in the object.

8. (Original) A method as recited in Claim 6, further comprising performing the inspecting periodically.

9. (Original) A method as recited in Claim 6, further comprising performing the inspecting during periods in which the data processing system is otherwise idle.

10. (Original) An apparatus for controlling access to an object in a data processing system, the apparatus comprising:

an access control data store for storing access control data associated with the object and the task; an access log;

access control logic for receiving a request to access the object from a task;

decision classifier logic, connected to the access control logic, the access control data store, and the access log, for classifying the access request into one of critical and non-critical classes in dependence on the access control data, and, in the event that the access is classified into the non-critical class, for granting the task access to the object and storing data indicative of the access in the access log; and,

access control decision logic connected to the access control logic, the access log, the access control data store, and the decision classifier logic, for, in the event that the access is classified into the critical class, granting or denying the task access to the object in dependence on the contents of the access log and the access control data.

11. (Original) An apparatus as recited in Claim 10, wherein, in use, the

decision classifier logic, in the event that the access is classified into the non-critical class, grants or denies the task access to the object in dependence on the contents of the access control data, and stores data indicative of the grant or denial in the access log.

12. (Original) An apparatus as recited in Claim 10, wherein the non-critical class comprises a plurality of subclasses and the decision classifier logic, in use, classifies the access request into one of the subclasses in dependence on the access control data.

13. (Original) An apparatus as recited in Claim 10, wherein the subclasses comprise a first subclass and a second subclass.

14. (Original) An apparatus as recited in Claim 13, wherein the decision classifier logic, in use, stores recovery data in the access log if the access is classified into the second subclass.

15. (Original) An apparatus as recited in Claim 14, wherein the access control decision logic, in use, inspects the access log to identify a bad grant decision based on the contents of the access log and the access control data, on detection of a bad grant decision, effects a roll back of any objects affected by the bad grant decision.

16. (Original) An apparatus as recited in Claim 15, wherein the rolling back comprises recovering data overwritten in the object.

17. (Original) An apparatus as recited in Claim 15, wherein the access control decision logic, in use, performs the inspection periodically.

18. (Original) An apparatus as recited in Claim 15, wherein the access control decision logic, in use, performs the inspection during periods in which the data processing system is otherwise idle.

19. (Original) Data processing system comprising:

a central processor unit;

a memory; and apparatus as recited in Claim 10 connected to the central processor unit and the memory.

20. (Previously Presented) A computer program product, the computer program product comprising:

a tangible storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method as recited in Claim 1.

21. (Previously Presented) An article of manufacture comprising a computer usable medium for storing computer readable instructions, which instructions, when processed by a data processing system, cause the data processing system to execute the steps set forth in the method of Claim 1.

22. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for controlling access to an object in a data processing system, said method steps comprising the steps of Claim 1.

23. (Previously Presented) A data processing system, the data processing system comprising an apparatus for controlling access to at least one object in the data processing system, wherein said apparatus is set forth in Claim 10.

IX. EVIDENCE APPENDIX

None. There is no evidence presented.

X. RELATED PROCEEDINGS APPENDIX

None. There are no related proceedings.

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. **20960**

In Re Application Of: **Morton G. Swimmer, et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/791,992	**March 3, 2004**	**Courtney D. Fields**	**45600**	**2137**	**4840**

Invention: **DATA PROCESSING SYSTEM**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:

The fee for filing this Appeal Brief is: **$510.00**

□ A check in the amount of the fee is enclosed.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0510/IBM. I have enclosed a duplicate copy of this sheet.

□ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **February 11, 2008**

John F. Vodopia
Registration No.: 36, 299

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza-Suite 300
Garden City, NY 11530
(516) 742-4343

~~I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on~~

~~*(Date)*~~

~~*Signature of Person Mailing Correspondence*~~

~~*Typed or Printed Name of Person Mailing Correspondence*~~

JFV:tb
cc: